Mobile Forensics

HOW BIOMETRIC AUTHENTICATION CREATES A CHALLENGE FOR MOBILE FORENSIC ANALYSTS

Zack Anderson | BSc Ethical Hacking | 14/10/2019

Smartphones are used as a hub for modern life; they contain passwords, authentication codes, online banking accounts, social media accounts, location information, messages, and much more personal and sensitive information. With all this information being gathered by their smartphone, consumers are becoming increasingly aware of the security features these devices offer to keep their information safe. However, this poses a problem for mobile forensic analysts, who will often struggle to gain access to download evidence from modern smartphones for cases where the information could be vital. This raises the topic question, "*What are the challenges faced by law enforcement in terms of mobile forensics?"* and how biometric authentication poses a potential challenge for mobile forensic analysts.

Since 2013, there has been a rising trend in the number of smartphones sold with various forms of biometric authentication. An estimated 71% of smartphones sold in 2018 featured biometric authentication in the form of fingerprint recognition (*Sharma, 2019*). These systems are quicker than typing a passcode and considered secure enough for online banking and payments on mobile devices, however, there are problems with these mechanisms. Firstly, they are inherently public – a password or phrase is only known by the user, whereas fingerprints and faces can be collected from impressions left on surfaces or high resolution photo and video recordings. Secondly, they cannot be changed meaning that if someone has their biometric data leaked, any biometric authentication they use becomes significantly less secure.

The most common type of biometric authentication on smartphones is the fingerprint sensor, as they are widely supported on mobile operating systems such as Android and iOS and, due to their simplicity compared to other methods such as facial authentication, relatively cheap. The popularity of this biometric authentication mechanism comes from its convenience for users, as they will always have the form of authentication immediately to hand and being very straightforward to use. There are 2 main methods of mainstream fingerprint recognition – in-display and capacitive.

Capacitive fingerprint sensors work by detecting the ridges of a fingerprint electrically using a capacitive surface. This works by detecting where the skin is contacting the surface as these areas will have a different resistance to areas without. This allows the sensor to detect characteristics such as the pattern, distance between ridges, and abnormalities (such as scars) in fingerprints. Since the sensor utilises the electronically conductive properties of human skin, it is less susceptible to cracking attempts and spoofing attacks.

In-display fingerprint scanners commonly use optical sensors, using light from the screen to create an image of the fingerprint (*Woodford, 2019*). The security of these sensors is debated among the cyber-security community, with one video showing a *Nokia 9* Android smartphone being unlocked with nothing more than a packet of chewing gum (*Nokia 9 Fingerprint unlocked with chewing gum, 2019*). Samsung developed an "*Ultrasonic"* in-display fingerprint scanner for their *Galaxy* and *Note* series of smartphones. This sensor uses ultrasonic pulses to build a 3D model of the users' fingerprint, measuring the depth of

troughs as well as data about the pattern and distance between ridges to theoretically provide a more secure in-display sensor than traditional capacitive methods (*Triggs, 2019*). However, Samsung's sensor was recently discovered to be flawed if the user had a thick or tempered glass screen protector on the phone, in which case the phone would unlock with any fingerprint. This has led to banking applications and other secure applications blacklisting the fingerprint scanner as a form of biometric authentication to access the application data (*Anderson*, 2019).

Another form of biometric authentication is facial recognition, which uses features of the user's face much in the same way as fingerprints, typically by utilising the phones front-facing camera. However, these systems are usually easily stumped by changing facial features such as glasses or beards. On top of using facial recognition, Samsung opted to develop an iris-scanning system for their phones which uses a specialised camera with an infrared LED to capture the iris pattern of the device user (*Arici, 2017*). It was discovered that the system was vulnerable to a spoofing attack involving a high-resolution photo of the victim's iris and a contact lens, which when overlaid, could fool the mechanism.

Some early versions of Google's Assistant allowed Android smartphones to be unlocked using a voice-unlock authentication mechanism before it was removed in Android version 9.0. The phone was trained on the users voice using the "*Ok, Google*" phrase to open the assistant, however, was deemed extremely insecure due to the systems inability to tell the difference between users voices, but also because of how easily a person's voice or accent can be impersonated, or even recorded (*Fisher, 2019*).

Google has outlined a testing methodology for testing biometric authentication in the official Android documentation which measures effectiveness by measuring two metrics; Imposter Acceptance Rate and Spoof Acceptance Rate (*Android Open Source Project*, 2019a). The imposter acceptance rate is the chance that the authentication mechanism accepts an input which is designed to imitate a correct sample, such as mimicking the users voice for voice unlock, while the spoof acceptance rate is the chance the mechanism will accept a previously recorded input, such as playing back the user saying the phrase to unlock the device using voice unlock. The documentation outlines how testing of authentication systems should be carried out in environments which mimic real-world scenarios on the hardware the device will use and setting up a robust testing mechanism. The tests outlined by the documentation include:

- Using high resolution photos that fill the camera sensor to fool facial authentication systems.
- Using fake fingerprints created using a mould using materials such as dental silicon.
- Testing the system against known vulnerabilities in similar systems.

Knowing how these systems are tested could allow attackers and mobile forensic analysts to identify possible vulnerabilities which they could exploit in order to gain access to a device.

Android performs biometric authentication checks in a Trusted Execution Environment (TEE) (*Hildenbrand, 2017*). A trusted execution environment is an isolated section of computational resources which may be virtualised on the main central processing unit (CPU) and memory or may operate as an independent system with its own hardware resources. The role of a TEE is to only allow authorised access to its data regardless of the other hardware and software modifications on the phone and as such it is not affected by the phone being rooted or the bootloader unlocked. Google calls the operating system that runs inside its virtualised TEE *Trusty OS* which, when queried, returns a true or false answer giving away no information to the software querying the environment to preserve the security of the data.

Trusty OS stores fingerprint data using "*templates"* which derive data from the users' fingerprint, meaning that the user's raw fingerprint data is not stored within the TEE. Android documentation also states that fingerprint enrolment, acquisition, and recognition must happen within the TEE, and that fingerprint templates must be signed with a private key that ensures only the intended user on the intended device can access the data (*Android Open Source Project, 2019b*). Fingerprint data also cannot be backed up or visible to any application, process, or user – even the root account. The implementation of the trusted execution environment depends on the hardware of the device. On ARM-based processors, *TrustyOS* runs on an isolated section of the CPU known as *"ARM TrustZone"* while on Intel this environment is virtualised using Intel's Virtualisation Technology.

The security of Android's facial recognition implementations has been debated since their conception. When first introduced in Android version 4.0 with a camera-based implementation, the system could be fooled simply using an image of the device owner. In version 4.1, they attempted to improve this by adding a "*liveness check"* which required the user to blink. However, this was also easily fooled by quickly switching between a photo of the user and a photoshopped image of them with their eyes closed (*Racoma, 2012*). Since then the security of Android's face unlock has improved with stricter guidelines outlined by Google, with Google's new Pixel 4 ditching the fingerprint sensor and exclusively using face unlock using a combination of radar, infrared, and camera sensors to authenticate the user. However, the current implementation has questionable security as it does not require any "*liveness checks"* aside from the infra-red camera, meaning that users can have their phones unlocked by someone while they are sleeping. Google have said they are planning to add this in an upcoming update (Keane, 2019).

The facial authentication is also carried out within a trusted execution environment and uses secure camera hardware to prevent injection attacks between the camera and the TEE. However, Android documentation also states that "*ideally, no process should have*

access except TEE and the hardware" indicating that it is not required and potentially easier to perform a man-in-the-middle attack on the mechanism.

Apple's fingerprint authentication mechanism, known as *"TouchID",* was used on iPhones up until the iPhone X and the same technology is still used on Apple's MacBook line-up of laptops today. Apple recommends using their fingerprint authentication system to users over the traditional 4-digit passcode which was previously standard on iOS. The 4-digit passcode would take on average 10,000 attempts to crack with simple passcodes such as "*1234"* being far simpler to guess, whereas Apple states "there is no such thing as a guessable fingerprint" and the odds of two peoples fingerprints being alike enough to successfully authenticate are roughly 1 in 50,000 (*Apple Inc.*, 2017a).

The "*TouchID*" authentication mechanism has some stricter rules compared to Android for when it requires password or passcode authentication rather than biometric authentication. The device will ask for an alternate method of authentication if:

- 48 hours have passed since the device was unlocked.
- Too many unrecognised attempts have been attempted through "*TouchID*".
- The device has restarted.
- Any security-related settings have been changed.

All biometric authentication within Apple devices is also executed and stored within a trusted execution environment known as the "*Secure Enclave"*. This is a standalone chip on all Apple devices rather than a virtualised environment as implemented on some Android devices. The data is stored as a mathematical representation of the biometric data; however, Apple is vague on the implementation of this storage mechanism on its devices.

Apple's facial authentication mechanism is known as "*FaceID"* – keeping with their conventional naming scheme for biometric authentication systems. "*FaceID"* is currently regarded as the most secure form of biometric authentication utilising Apple's "*TrueDepth*" camera system which allows the device to map out the geometry of the users face and construct a depth map using an infra-red camera and 30,000 points of reference (*About Face ID advanced technology*, 2019). Apple has stated that the odds of a person's face successfully authenticating on another person's device is roughly 1 in 100,000 – theoretically making it more secure than Apple's old "*TouchID"* system.

The mechanism mainly focuses on features around the users' eyes, nose, and mouth, but is also able to deal with changes in facial features which many of its Android competitors cannot – such as the user wearing glasses or growing facial hair. *"FaceID*" also requires the user to look at the phone for it to unlock to ensure the user is deliberately unlocking the device and performs liveness checks such as looking for movements in the pupils of the user to ensure an attacker is not trying to imitate the users facial features. *"FaceID"* also

uses the "*Secure Enclave"* system to execute and store mathematical representations of biometric data on the device, meaning no facial data is stored on the device storage.

iOS and Android also utilise encrypted storage mechanisms which decrypt the system partition to boot the device, then the user partition after the user first unlocks the device. On Android, it uses a mechanism called *Direct Boot* to encrypt files and decrypt necessary system files on boot stored in the *Device Encrypted Storage* partition. However, waits until after the user unlocks the device before decrypting all other files stored in the *Credential Encrypted Storage,* which is encrypted using the users passcode, password, or pattern lock (*Android Developers,* 2019c). If the user uses complex passwords or passcodes, this can make it difficult for forensic mobile forensic analysts to brute force, meaning they may turn to attack the biometric sensors rather than the user credentials.

On Android and iOS devices, the user is required to enter their user credentials when the device is first booted rather than relying on biometrics to decrypt the user storage on the device. This poses an issue for mobile forensic analysts as they cannot unlock the device using biometrics if the device was powered off when it is acquired and cannot read any data on the device without the password or passcode. Apple devices also have the added caveat of requiring an alternate method of authentication to biometrics if the device hasn't been unlocked for 48 hours. This puts a time limit on the time attackers have to try and unlock the device by spoofing biometric mechanisms, however, also adds a challenge for authorities.

The high level of protection on biometric authentication mechanisms and biometric data, combined with other precautions implemented by companies to stop spoofing attacks, means that it simply does not make sense for mobile forensic analysts to attack biometric systems outside of a few limited use cases. Security on other parts of the device are likely weaker, especially if the phone is running older software which may have vulnerabilities which could give access to the files on the device without needing to use biometric authentication or cracking passcodes – which could take a long time depending on the age of the device and subsequently its biometric hardware, and the complexity of any passwords or passcodes. There are, however, a few exceptions to this conclusion. Some Android smartphones used fingerprint scanners before Google officially added native support and protocols for the feature in Android 6.0. Devices with biometric authentication which ran on Android versions below 6.0 used manufacturers own protocols, a lot of which were scarily insecure. The Samsung Galaxy S5 was vulnerable to an attack which allowed an attacker to extract fingerprint data from the device storage, while the HTC One Max stored the fingerprint, uncompressed and unencrypted, as an image on the phones storage, without modifying permissions which meant any process or user on the phone could see the image.

In an interview in 2017, Travis Jarae, CEO of privacy research company *OneWorldIdentity*, stated that courts in the United States may be able to force a suspect to unlock their phone using biometrics as "attributes of the body are not protected under the fifth

amendment" (*Bonnington*, 2017). While authorities cannot currently force you to hand over passwords or passcodes for devices (although they can hold you in prison until you do) – biometrics do not fall under this category. Apple chose to implement a 48-hour counter for their biometric authentication – after which, the device will require a password – which gives attackers less time after stealing a device to attempt a reconstruction of any biometrics of the victim, but also may stop authorities forcing a suspect to unlock their phone.

In the UK the laws are different, and a suspect can be sentenced for refusing to give passwords to the authorities to aid an active investigation under the Regulation of Investigatory Powers Act 2000 (*Vaas*, 2018). Police must apply for and obtain a court order to request the information from the suspect, and only then can they charge someone under the Regulation of Investigatory Powers Act. The maximum sentence someone can be given for a violation of this act is 2 years, extended to 5 if the subject is a matter of national security or child endangerment.

Manufacturers also cannot provide authorities with access to devices they manufacture due to their security implementations. Apple were thrown into the spotlight after the San Bernardino shootings took place in the United States for refusing to unlock an iPhone used by one of the shooters, with Apple CEO Tim Cook saying unlocking the phone would "set a dangerous precedent" (*Holpuch*, 2016). This led to a debate on if authorities should have backdoors into devices such as smartphones for forensic purposes for matters of national security. However, there would be nothing stopping other attackers with malicious intent from also finding and utilising these backdoors.

References

Nokia 9 Fingerprint unlocked with chewing gum (2019). Available at: https://www.youtube.com/watch?v=hSlotw4WHDA (Accessed: 15 October 2019).

Measuring Biometric Unlock Security | Android Open Source Project (2019a). Available at: https://source.android.com/security/biometric/measure (Accessed: 4 November 2019).

Fingerprint HIDL | Android Open Source Project (2019b). Available at: https://source.android.com/security/authentication/fingerprint-hal (Accessed: 21 October 2019).

Support Direct Boot mode | Android Developers (2019c). Available at: https://developer.android.com/training/articles/direct-boot (Accessed: 15 October 2019).

About Touch ID advanced security technology (2017a). Available at: https://support.apple.com/en-gb/HT204587 (Accessed: 4 November 2019).

About Face ID advanced technology (2019b). Available at: https://support.apple.com/en-gb/HT208108 (Accessed: 4 November 2019).

Anderson, T. (2019) "Any finger will do? Samsung Galaxy S10 with a screen protector reportedly easy to fool". Available at: https://www.theregister.co.uk/2019/10/17/samsung_galaxy_s10_note_10_fingerprint_bypass/ (Accessed: 4 November 2019).

Arici, A. (2017) *How does the Samsung Galaxy S8 iris scanner work?*, *AndroidGuys*. Available at: https://www.androidguys.com/featured/how-does-the-samsung-galaxy-s8-iris-scanner-work/ (Accessed: 21 October 2019).

Bonnington, C. (2017) "Apple Plans to Share Some Data That the iPhone X Collects About Your Face. That's a Huge Worry.", *Slate.com*. Available at: https://slate.com/technology/2017/11/apple-plans-to-share-some-iphone-x-face-id-data-uh-oh.html (Accessed: 4 November 2019).

Fisher, C. (2019) *'OK Google' will no longer fully unlock your phone*, *Engadget.com*. Available at: https://www.engadget.com/2019/03/01/ok-google-voice-match-unlock-update/ (Accessed: 21 October 2019).

Hildenbrand, J. (2017) *How does Android save your fingerprints?*, *Android Central*. Available at: https://www.androidcentral.com/how-does-android-save-your-fingerprints (Accessed: 21 October 2019).

Holpuch, A. (2016) "Tim Cook says Apple's refusal to unlock iPhone for FBI is a 'civil liberties' issue". Available at: https://www.theguardian.com/technology/2016/feb/22/tim-cook-apple-refusal-unlock-iphone-fbi-civil-liberties (Accessed: 4 November 2019).

Keane, S. (2019) "Pixel 4's Face Unlock will work even if you're dead, and Google says a patch is months away", *CNet*. Available at: https://www.cnet.com/news/pixel-4-face-unlock-works-even-when-your-eyes-are-closed-unconscious-dead-google-patch-months-away/ (Accessed: 5 November 2019).

Racoma, J. (2012) *Android Jelly Bean Face Unlock 'liveness' check easily hacked with photo editing*, *Android Authority*. Available at: https://www.androidauthority.com/android-jelly-bean-face-unlock-blink-hacking-105556/ (Accessed: 22 October 2019).

Sharma, P. (2019) "More Than One Billion Smartphones with Fingerprint Sensors Will Be Shipped In 2018", *Counterpoint*. Available at: https://www.counterpointresearch.com/more-than-one-billion-smartphones-with-fingerprint-sensors-will-be-shipped-in-2018/ (Accessed: 15 October 2019).

Triggs, R. (2019) "Ultrasonic fingerprint scanners: how do they work?", *Android Authority*. Available at: https://www.androidauthority.com/how-do-ultrasonic-fingerprint-scanners-work-666053/ (Accessed: 15 October 2019).

Vaas, L. (2018) "How refusing to give police your Facebook password can lead to prison", *naked security*. Available at: https://nakedsecurity.sophos.com/2018/09/04/how-refusing-to-give-police-your-facebook-password-can-lead-to-prison/ (Accessed: 4 November 2019).

Woodford, C. (2019) *How do fingerprint scanners work*, *Explain that Stuff*. Available at: https://www.explainthatstuff.com/fingerprintscanners.html (Accessed: 15 October 2019).